UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,517	09/30/2003	Jeffrey A. Aaron	9400-150	6101

39072 7590 02/17/2010

AT&T Legal Department - MB
Attn: Patent Docketing
Room 2A-207
One AT&T Way
Bedminster, NJ 07921

EXAMINER	
TIMBLIN, ROBERT M	
ART UNIT	PAPER NUMBER
2167	
MAIL DATE	DELIVERY MODE
02/17/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/675,517	AARON ET AL.	
	Examiner	Art Unit	
	ROBERT TIMBLIN	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/24/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office action corresponds to application 10/675,517 which was filed 9/30/2003.

Response to Amendment

Applicant herein amends claims 1, 10, and 18. Claims 1-20 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-20 are rejected under.35 USC 103(a) as being obvious over Vinberg (U.S. 2003/0023722 A1), in view of Sands (Sands et al. U.S. 2004/0148526 A1).

Regarding claim 1, Vinberg discloses a method of outputting an alert indicating that an event has occurred, the method comprising:

obtaining a status from a sensor (Figure 3A, elements 305-319., paragraph 0009 and 0030; e.g. alert condition detector; status information from each element is the equivalent of status from a sensor, see also element 120),

generating the alert (Figure 4, element 410, paragraph 0050);

applying a filter (0038; e.g. the importance property [of the alert] represents a measure of the importance of the object) to determine whether to modify (0038; e.g. assigning a severity property) a severity (0035, 0038; e.g. importance and "mission critical" level) of the alert (Figure 4, element 420, paragraph 0053, see also paragraph 0028; e.g. alert filter and whether to report an alert condition), and outputting the alert (Figure 4, element 430, paragraph 0053; e.g. generate output alert).

Vinberg does not explicitly disclose wherein the event is unauthorized, and retrieving personnel information comprising identity and status information for the personnel from a database, the personnel information relating to the sensor and the status information comprises job category and/or authorized access zone information.

In the same field of endeavor (alerts in response to detection of an event) Sands discloses wherein the event is unauthorized (elements 455 and 465, paragraphs 0083 and 0085), and retrieving personnel information comprising identity (figures 3 and 4 and descriptions of starting at paragraph 0067, a user ID within a biometric profile is disclosed (corresponding to *identity information)* and status (e.g. 420 of figure 4 and paragraph 0073 discloses that a location may be disabled (corresponding to *status information)* information from a database (100, 205), the personnel information relating to the sensor (Figure 4, elements 410 and 435 wherein a sensor (e.g. 400-405 uses personnel information), paragraphs 0069 and 0076) and the status information comprises job category (i.e. table beneath 0095; "Admin" being a job category) and/or authorized (0028; e.g. detecting an imposter attempting to gain access to unauthorized resources - the resources seen as an example of a zone; also 0073 describes enabled/disabled locations which are seen as authorized access zones, further, 0036 and fig. 2 teaches that the authentication

server comprises an authentication policy that defines what the requirements are for authenticating a user at each location (interpreted as "zone") on the computer network) access zone information (415; e.g. retrieving configuration info for a location 0073); e.g. certain locations may be disabled regardless of who is logging in. Therein the indication of disabled locations may be access zone information).

Accordingly, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Sands' teachings of detection of an unauthorized event and retrieving personnel information from a database with Vinberg's teachings of alert generation to obtain the disclosed limitations. Sands suggests in paragraph 0085 that actions need to be taken in the event of conditions relating to the personnel information of the database. Vinberg suggests monitoring and managing ongoing processes in paragraph 0002, and in paragraph 0050 that any condition known
to one of skill in the and may be used in the detection of alert conditions.

Regarding claim 2, further comprising retrieving information relating to a prior event from the database, Vinberg teaches in paragraph 0042 the use of an alert condition, database, which a filter module processes events that have been stored prior to processing. In this instance alert conditions objects are the equivalent of prior events.

Regarding claim 3, further comprising accumulating the alert, (Vinberg, paragraph 0038 and 0048; e.g. alert severity).

Regarding claim 4, further comprising re-evaluating the severity of the alert, Vinberg teaches in paragraph 0025 the use of an automatic discovery utility that can be used to continually monitor the status of components in a system (the equivalent of sensors). The evaluation of a severity of an event, discussed in paragraph 0026, is continuously evaluated and re-evaluated.

Regarding claim 5, further comprising re-evaluating the uncertainty of the alert, Vinberg teaches in paragraph 0025 the use of an automatic discovery utility that can be used to continually monitor the status of components in a system (the equivalent of sensors. The evaluation of the uncertainty of an event, (called likelihood in Vinberg) is discussed in paragraph 0026, and is continuously evaluated and re-evaluated.

Regarding claim 6, further comprising applying a filter to determine whether to limit outputting of the alert (Vinberg, paragraph 0053).

Regarding claim 7, further comprising outputting a recommendation relating to the alert, Vinberg teaches the limitation in the disclosure of a warning in paragraph 0050. A warning is a recommendation to an operator to consider the effects of a message sent from a device.

Regarding claim 8, wherein obtaining a status from a sensor includes obtaining a status from one of an infrared sensor, a physical sensor, a motion detection senor, aireless sensor, an audio pattern recognition device, a video pattern recognition device, a card reader, a biometric

sensor, a software monitoring device, a trip wire, an electric eye, a pressure sensor, an access panel switch, a door switch, a microwave sensor, and a System Network Management Protocol (SNMP) trap source/event message, Sands discloses the use of a biometric sensor in paragraph 0023 et seq. The same motivation to combine the teachings of Sands and Vinberg applied in claim 1 applies equally as well to the rejection of claim 8.

Regarding claim 9, wherein outputting the alert includes outputting one of a telephone message, an electronics message, a paper message, a visual indication, and an auditory indication, Vinberg discloses in paragraph 0022 a visualization workstation (element 105) that gets notification of events, which are the equivalent of a visual indication.

Regarding claim 10, Vinberg discloses a system for outputting an alert, the system comprising:

a sensor interface (Figure 3A, elements 305-319, paragraph .0030; status information from each element is the equivalent of status from a sensor', see also element 120);

a database (element 110, paragraph 0023);

an alert processor in communication with the sensor interface and the database (paragraph 0024, element 1 15), wherein the alert processor is configured to retrieve personnel information from the database, generate the alert (Figure 4, element 410, paragraph 0050)', apply a filter to determine whether to modify the severity of the alert (Figure 4, element 420, paragraph 0053, see also paragraph 0028), and output the alert (Figure 4, element 430, paragraph 0053).

Vinberg does not explicitly disclose retrieving personnel information from the database, the personnel information comprises identity and status information for the personnel and is related to the sensor and the status information comprises job category and/or authorized access zone information.

In the same field of endeavor (alerts in response to detection of an event) Sands discloses retrieving personnel information from a database, the personnel information comprises identity (figures 3 and 4 and descriptions of starting at paragraph 0067, a user ID within a biometric profile is disclosed (corresponding to *identity information)* and status (e.g. 420 of figure 4 and paragraph 0073 discloses that a location may be disabled (corresponding to *status information)* from the database (100, 205) information for the personnel and is related to the sensor (Figure 4, elements 410 and 435, paragraphs 0069 and 0076) and the status information comprises job category (i.e. table beneath 0095; "Admin" being a job category) and/or authorized (0028; e.g. detecting an imposter attempting to gain access to unauthorized resources - the resources seen as an example of a zone; also 0073 describes enabled/disabled locations which are seen as authorized access zones, further, 0036 and fig. 2 teaches that the authentication server comprises an authentication policy that defines what the requirements are for authenticating a user at each location (interpreted as "zone") access zone information (0073; e.g. certain locations may be disabled regardless of who is logging in. Therein the indication of disabled locations may be access zone information).

Accordingly, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Sands' teachings of detection of an unauthorized event and retrieving personnel information from a database with Vinberg's teachings of alert

generation to obtain the disclosed limitations. Sands suggests in paragraph 0085 that actions need to be taken in the event of conditions relating to the personnel information of the database. Vinberg suggests monitoring and managing ongoing processes in paragraph 0002, and in paragraph 0050 that any condition known to one of skill in the art may be used in the detection of alert conditions.

Regarding claim 11, wherein the alert processor includes an alert generation module (Vinberg, figure 2, element 220, paragraph 0037).

Regarding claim 12, wherein the alert processor includes an input module, Vinberg teaches in Figure 3C messages coming from a plurality of disparate devices (Figure IB, element 115). It was obvious to a person of ordinary skill in the art at the time the invention to use management application 1 15 to format objects created from system events into a format readable by other components of the system.

Regarding claim 13, wherein the alert processor includes a filter module (Vinberg, figure 2, element 230, paragraph 0042).

Regarding claim 14, wherein the alert processor includes an alert uncertainty and severity estimation module (Vinberg, figure 2, element 230, paragraph 0048).

Regarding claim 15, wherein the alert processor includes a rule and algorithm update module (Vinberg, figure 2, element 205, paragraph 0027).

Regarding claim 16, wherein the alert processor includes a filter/mode selection module (Vinberg, figure 2, element 205, paragraph 0027). Paragraph 0027 of Vinberg details a module that provides access and modification to objects in the system enabling an operator to define criteria under which alert notifications may be reported. The filter criteria maintenance module then meets the limitations of both a rule and algorithm update module and a filter/mo' de selection module.

Regarding claim 17, wherein the alert processor includes an alert output module (Vinberg, figure 2, element 235, paragraph 0043).

Regarding claim 18, Vinberg teaches A computer readable medium having stored thereon instructions which, when executed, cause a processor to:

obtain a status from a sensor (Figure 3A, elements 305-319., paragraph 0009 and 0030; e.g. alert condition detector; status information from each element is the equivalent of status from a sensor, see also element 120),

generate the alert (Figure 4, element 410, paragraph 0050);

apply a filter to determine whether to modify a severity of the alert (Figure 4, element 420, paragraph 0053, see also paragraph 0028; e.g. alert filter), and output the alert (Figure 4, element 430, paragraph 0053; e.g. generate output alert).

Vinberg does not explicitly disclose wherein the event is unauthorized, and retrieving personnel information comprising identity and status information for the personnel from a database, the personnel information relating to the sensor and the status information comprises job category and/or authorized access zone information.

In the same field of endeavor (alerts in response to detection of an event) Sands discloses wherein the event is unauthorized (elements 455 and 465, paragraphs 0083 and 0085), and retrieving personnel information comprising identity (figures 3 and 4 and descriptions of starting at paragraph 0067, a user ID within a biometric profile is disclosed (corresponding to *identity information)* and status (e.g. 420 of figure 4 and paragraph 0073 discloses that a location may be disabled (corresponding to *status information)* information from a database (100, 205), the personnel information relating to the sensor (Figure 4, elements 410 and 435 wherein a sensor (e.g. 400-405 uses personnel information), paragraphs 0069 and 0076) and the status information comprises job category (i.e. table beneath 0095; "Admin" being a job category) and/or authorized (0028; e.g. detecting an imposter attempting to gain access to unauthorized resources - the resources seen as an example of a zone; also 0073 describes enabled/disabled locations which are seen as authorized access zones, further, 0036 and fig. 2 teaches that the authentication server comprises an authentication policy that defines what the requirements are for authenticating a user at each location (interpreted as "zone") access zone information (0073; e.g. certain locations may be disabled regardless of who is logging in. Therein the indication of disabled locations may be access zone information).

Accordingly, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Sands' teachings of detection of an unauthorized

event and retrieving personnel information from a database with Vinberg's teachings of alert generation to obtain the disclosed limitations. Sands suggests in paragraph 0085 that actions need to be taken in the event of conditions relating to the personnel information of the database. Vinberg suggests monitoring and managing ongoing processes in paragraph 0002, and in paragraph 0050 that any condition known to one of skill in the art and may be used in the detection of alert conditions.

With respect to claim 19, Sands discloses the computer readable medium of claim 18, having stored thereon additional instructions that cause the processor to obtain a status from one of an infrared sensor, a physical sensor, a motion detection sensor, a wireless sensor, an audio pattern recognition device, a trip wire, an electronic eye, a pressure sensor, an access panel switch, a door switch, a microwave sensor, and a System Network Management Protocol (SNMP) trap source/event message as a biometric sensor in paragraph 0023 et seq. The same motivation to combine the teachings of Sands and Vinberg applied in claim 1 applies equally as well to the rejection of claim 18.

With respect to claim 20, Sands discloses he computer readable medium of claim 18, having stored thereon additional instructions that cause the processor to output one of a telephone message, an electronic message, a pager message, a visual indication, and an auditory indication (105 e.g. displaying event notifications).

Response to Arguments

Applicant's arguments filed 11/24/2009 have been fully considered but they are not persuasive.

Applicant argues on page 7 of the reply that Sands does not provide any description of including an administrator designation for personnel in the storage medium 205. Examiner respectfully disagrees given the following:

As noted in the rejection above, Sands teaches maintaining system permissions information that comprises associating a user in a group (see Sands, paragraph under 0095 – Admin). More specifically, Sands discloses associating a user within a group such as an administrative group. Therein by this association, Examiner submits that Sands discloses a user as an administrator, which is seen as a job category, for personnel. Further, since the authentication server (which includes database 205) retrieves this information (i.e. recognizes that the user is an administrator) it is seen to store this status information that comprises a job category for personnel. Furthermore, Examiner submits that information regarding a user as an administrator describes a user profile. Sands discloses that a user profile is stored in memory (e.g. see 0014 and 0054) and thus the claimed status information of a job category for personnel is stored in a database is taught.

With respect to the status information comprising authorized access zone information, Applicant argues on page 8 that Sands does not anticipate specifying authorized access zones for personnel in a database. Examiner respectfully disagrees given the following:

As given in figure 4, Sands discloses the authentication server retrieving information for a location (415) and thereafter determines if the location has been disabled (420). Thus,

Examiner submits from the retrieved information, Sands teaches that the location, or "zone" can be accessed. Accordingly, Examiner submits that because information indicating if a location is enabled/disabled is retrieved by a server, that Sands discloses the authorized access zone as claimed. In other words, the authentication server is seen to contain information regarding locations and their status (enabled/disabled) that indicate if they are authorized access zones for users (i.e. personnel).

Furthermore, Sands teaches the authentication server comprises an authentication policy (see fig. 2) that defines what the requirements are for authenticating a user at each location (interpreted as "zone") on the computer network (see 0036). Moreover, Examiner submits that such a policy further identifies a user as an administrator (see table under 0095) and also indicates a job category for the personnel. Therein, Sands is further seen to teach that status information for the personnel including authorized access zone information is stored in a database.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert M. Timblin whose telephone number is 571-272-5627. The examiner can normally be reached on M-Th 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ROBERT TIMBLIN/

Examiner, Art Unit 2167

/John R. Cottingham/

Supervisory Patent Examiner, Art Unit 2167